EXHIBIT B-1

Fig. 1

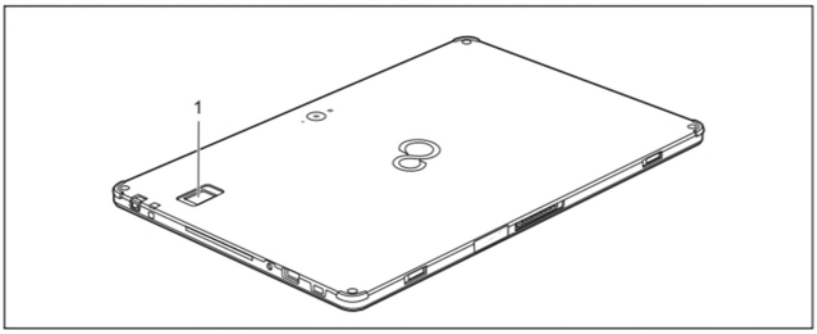
User Security	Embedded fingerprint sensor (optional) Smartcard reader (optional) Hard disk password User and supervisor BIOS password SystemLock BIOS SmartCard security Workplace Protect (secure authentication solution)

Fig. 2

Configuring the fingerprint sensor (configuration dependent)

Whether your device has a fingerprint sensor or not depends on the device configuration which you ordered.

The fingerprint sensor can record the image of a fingerprint. With additional fingerprint software, this image can be processed and used instead of a password.



► Install the fingerprint software to be able to use the fingerprint sensor (1).

Fig. 3

Make fingerprint settings

No fingerprints can be recorded for user accounts which were automatically created by Windows 8 (Administrator, Guest). An error message appears in this case.

The first steps differ, depending on the pre-set Authentication Level.

Single-Factor Authentication	If this method is set, the images are saved on the computer.
Multi-Factor (Template on Card)	If this method is set for identification on the system, the images are saved on the smartcard. ► Insert the smartcard into the reader before starting to scan. **NOTE**: If you work on different computers with the smartcard, you must save palm-vein images on the smartcard for each system.
Multi-Factor (Secret)	If this method is set for identification on the system, the first time the palm-vein imaging is set up, the user is automatically requested to enter the secret first. ► Enter the secret and click *activate*.

► Under *security devices*, click *fingerprint | start wizards*.
► Confirm with *Next*.
► When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").
► Select the finger for which you would like to perform an action.
► Click on the button of the desired action:

Action	Description
Record	Read in and save fingerprint
Verify	Verify fingerprints already saved
Remove	Delete fingerprints already saved
Back	Back to the choice of finger

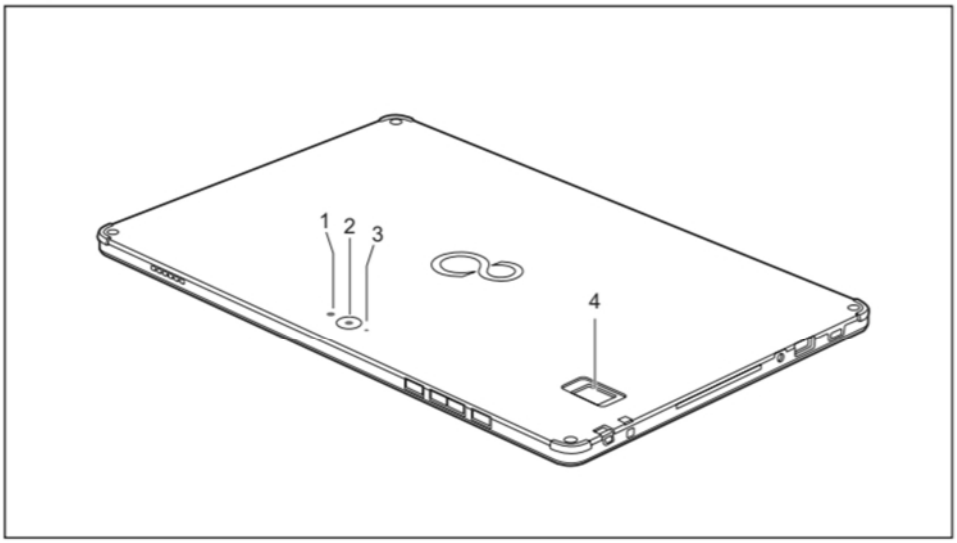
Read in fingerprint

At least two fingerprints must have been read in and stored before you can end the configuration.

► In the menu bar, click on *Security Devices - Fingerprint*.
► Select one finger by clicking in the circle above the desired finger.
The circle above the finger will be marked in blue.
► Click on *Record*.
► Draw the desired finger evenly over the fingerprint sensor.
Four successful recordings must be made to complete the process.

Fig. 4

Rear



1 = Camera light
2 = Camera
3 = Camera LED
4 = Fingerprint sensor (configuration dependent)

Fig. 5

Setting the security devices

Only *security devices* that are supported by the system can be selected.

In managed mode, only devices and combinations that have been approved by the administrator are displayed.

If Multi-Factor Authentication is set on the system, the associated methods must also be configured when selecting a security device. Possible combinations are:

- Fingerprint or palm veins and smartcard
- Palm veins or fingerprint or face recognition or RFID and additional password (secret)

Under *security devices*, the following functions are available to you:

Security device	Icon	Description
PalmSecure™		Save palm images, verify or delete those already saved
Fingerprint		Save fingerprints, verify or delete those already saved
Face recognition		Configure face recognition
Presence sensor		Change the settings of the presence sensor
Passwords		Manage passwords for Windows, BIOS and hard drives
SmartCard / RFID		Configure SmartCard or RFID card

You can call up a function either using the menu bar or by clicking on the relevant icon in the display area.

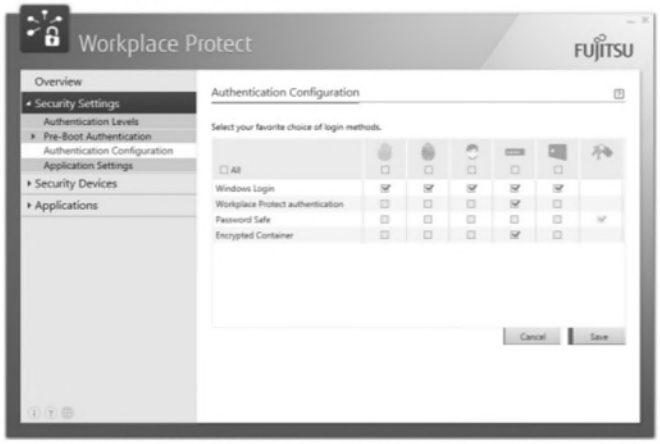
If you call up the function with start wizards, a wizard guides you through the settings. In the wizard you will find further information and additional background knowledge.

Fig. 6

Authentication configuration

To make settings in the authentication configuration, proceed as follows:

- ► Under *Security Settings*, click on *Authentication Configuration*.
- ► When you are asked, authenticate yourself to the system (see chapter "Perform the necessary authentication in Workplace Protect").



- ► For the authentication methods, check the checkbox for the desired security devices to be able to use them for authentication.

Function	Description
All	Marks all possible authentication methods
Windows logon	Settings for the supported authentication methods during Windows logon
Workplace Protect authentication	The authentication settings specified here will always be used to authenticate the user for the configuration of security devices and security settings.
Password Safe	User authentication for Password Safe
Encrypted Container	User authentication for the Encrypted Container

Fig. 7

Protecting BIOS Setup Utility (supervisor password and user password)

If you have opened these operating instructions on the screen, we recommend that you print them out. You cannot call up the instructions on the screen while you are setting up the password.

The supervisor password and the user password both prevent unauthorized use of the *BIOS Setup Utility*. The supervisor password allows you to access all of the functions of the *BIOS Setup Utility*, while the user password will only give you access to some of the functions. You can only set up a user password if a supervisor password has already been assigned.

Calling and using the *BIOS Setup Utility* is described in the chapter "Settings in BIOS Setup Utility", Page 82.

Assigning the supervisor and user passwords

- ► Start the *BIOS Setup Utility* and go to the *Security* menu.
- ► Select the *Set Supervisor Password* field and press the Enter key.
- ↳ With *Enter new Password*: you are asked to enter a password.
- ► Enter the password and press the Enter key.
- ↳ *Confirm new Password* requires you to confirm the password.
- ► Enter the password again and press the Enter key.
- ↳ *Changes have been saved* is displayed as a confirmation that the new password has been saved.
- ► To set the user password, select *Set User Password* and proceed exactly as when configuring the supervisor password.
- ↳ If you do not want to change any other settings, you can exit *BIOS Setup Utility*.
- ► In the *Exit* menu, select the option *Save Changes & Exit*.
- ► Select *Yes* and press the Enter key.
- ↳ The Tablet PC is rebooted and the new password is effective. It will now be necessary to first enter your supervisor or user password in order to open the *BIOS Setup Utility*. Please note that the user password only provides access to a few of the BIOS settings.

Changing the supervisor password or user password

You can only change the supervisor password when you have logged into the *BIOS Setup Utility* with the supervisor password.

- ► Start the *BIOS Setup Utility* and go to the *Security* menu.
- ► When changing the password, proceed exactly as when assigning a password.

Fig. 8

Smartcard

Insert the smartcard

When you insert the smartcard into the reading device, one of the following symbols may appear.

Symbol	Meaning
	The smartcard is valid and contains login details.
	The status of the smartcard is unknown. The smartcard must be unlocked using the PIN.
	The smartcard is not supported.

Configuring a SmartCard

- ► In the menu bar, click on *Security Devices - SmartCard / RFID*.
- ► Insert the SmartCard into the module provided.

A wizard with further information on the functionality is shown.

- ► Follow the instructions on the screen.

A summary of the settings you have made is displayed.

- ► Confirm with *Finish*.

You then return to the overview page.

Fig. 9

Changing the SmartCard settings

Proceed as follows to make changes to the SmartCard settings:

- ► In the menu bar, click *Security Devices - SmartCard / RFID.*
- ► Insert the SmartCard into the module provided.
- ► Follow the instructions on the screen.

You arrive at the overview page showing the SmartCard settings.

You can make the following settings here:

Tab	Function
Admin	Activate SystemLock (see chapter "Activate and configure SystemLock")
Change PIN	Change current PIN
Change PUK	Change current PUK
Unblock PIN	Unblock PIN which has been blocked
User management	Delete registered users on the SmartCard
SystemLock cards	Write access data for SystemLock onto SmartCards

► To make changes to the settings, click on the corresponding tab at the upper edge of the

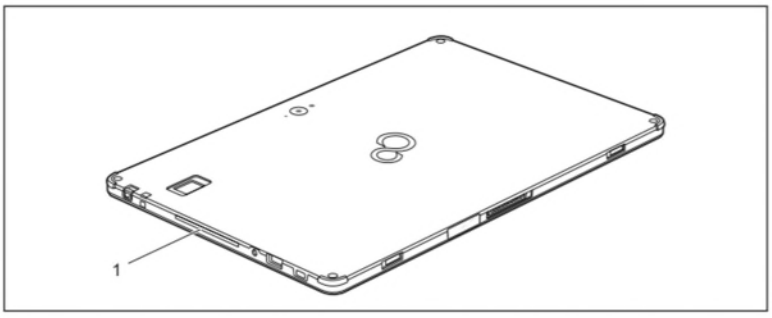
Fig. 10

Inserting the SmartCard

Your device may be fitted with a Smart Card reader, depending on your chosen model (only available in models with screw holes and Smart Card reader).

Do not use force when inserting and removing the SmartCard.

Make sure that foreign objects do not fall into the SmartCard reader.



► Slide the Smart Card into the Smart Card reader (1) with the chip facing the front of the Tablet PC.

Fig. 11


Compare
STYLISTIC® Q739 Hybrid Tablet PC
13.3" Advanced Hybrid Convertible Tablet PC
Starting Configuration
Starting Price $1,599
Customize
Processor
8th Generation Intel® Core® i5-8365 Processor, 6 MB, Up to 4.1 GHz with Intel® Turbo Boost Technology
Operating System
Windows® 10 Pro (MUI) 64-bit
Display
13.3", Widescreen; LED backlight, bright LCD with wide viewing angles, FHD, 1920 x 1080, Capacitive touch panel with Wacom® Active ES pen (2048 pressure levels)
Graphics
Intel® UHD 620 Graphics, Shared
System Memory
8 GB (8GB x 1), Up to 16 GB Total, 2133 MHz, LPDDR3
Hard Drive
128 GB[1], M.2 SATA SSD

Fig. 12

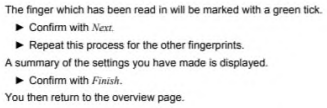

The finger which has been read in will be marked with a green tick.
► Confirm with Next.
► Repeat this process for the other fingerprints.
A summary of the settings you have made is displayed.
► Confirm with Finish.
You then return to the overview page.

Fig. 13

Security functions

Your Tablet PC has several security features that you can use to secure your system and your personal data from unauthorized access.

This chapter explains how to use these functions, and what the benefits are.

Please remember that in some cases, for example, forgetting your password, you may be locked out of the system and unable to access your data. Therefore, please note the following information:

- Back up your data on external data carriers at regular intervals.
- Some security functions need you to choose passwords. Make a note of the passwords and keep them in a safe place.

If you forget your passwords you will need to contact our Service Desk. Deletion or resetting of passwords are not covered by your warranty and a charge will be made for assistance.

In the BIOS setup utility menu *Security*, if you alter the *Password Severity* setting from its delivery status of *Strong* to *Stringent*, the Fujitsu Service Desk will no longer be able to reset the password. The system may then remain unusuable indefinitely.

Fujitsu therefore recommends always setting up a Supervisor password with the setting of *Password Severity* = *Strong*.

Fig. 14